White Paper: **January 2023**

# Put the Hybrid Cloud to Work for You: VMware Cloud on AWS

## Table of contents

### The struggle to find the right cloud skillsets

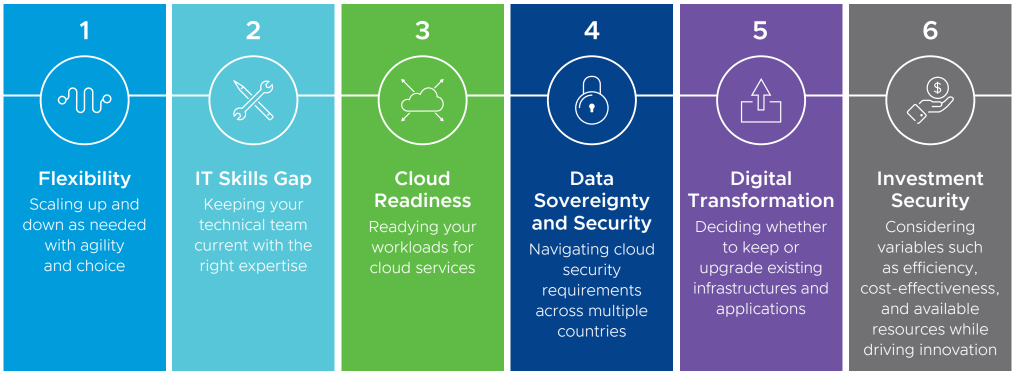
**85%**

of organizations are facing skills shortages in cloud expertise, an obstacle to optimal cloud execution.[1]

## Executive summary

Moving to the public cloud offers your organization some unquestionable and very attractive benefits. But there are definite challenges along the way that are as unique as the workloads you run and how much of your on-premises operations you want to move to the public cloud. This paper will help you assess your own cloud readiness and present why VMware Cloud™ on AWS is an optimal solution to consider when it comes to modernizing and future-proofing your existing applications.

## The six challenges to achieving desired cloud outcomes



1 **Flexibility** Scaling up and down as needed with agility and choice

2 **IT Skills Gap** Keeping your technical team current with the right expertise

3 **Cloud Readiness** Readying your workloads for cloud services

4 **Data Sovereignty and Security** Navigating cloud security requirements across multiple countries

5 **Digital Transformation** Deciding whether to keep or upgrade existing infrastructures and applications

6 **Investment Security** Considering variables such as efficiency, cost-effectiveness, and available resources while driving innovation

**Figure 1:** The 6 challenges to achieving desired cloud outcomes

### 1. Flexibility

It's important that your technology teams have flexibility and options when it comes to implementing your cloud strategies. They must be able to choose hardware, operating systems, platforms and deployment options in the private or public cloud in order to be responsive and agile to the demands of your business and be able to scale up or down depending on capacity needs. The cloud plays an important role in helping them deliver capacity rapidly and provide an avenue for modernizing your existing enterprise applications. However, when it comes to transforming your on-premises applications, there are serious concerns about increased costs, security risks and downtime during migration and modernization efforts.

### 2. IT skills gap

The single largest barrier for technology teams looking to build a proper cloud strategy is the growing IT skills gap regarding cloud technologies. It's even worse for organizations that want to modernize their existing applications. You could potentially be putting your organization at risk if your current technical team doesn't possess the right expertise and you can't find people who do. Whether you're trying to figure out how public cloud providers should approach virtual machine (VM) migration, rewrite VM and application availability and security policies, learn how to cost-effectively manage workloads in these architectures, or modernize applications — many organizations are struggling to get things done with their existing teams because of the shortage of skilled IT workers in the job market.

[1] 451 Research, part of S&P Global Market Intelligence, Voice of the Enterprise (VotE): Cloud, Hosting & Managed Services, Organizational Dynamics 2020.

IDC found that only

9%

of customers rewrite or refactor applications when they shift them to the cloud.[2]

### 3. Cloud readiness

While addressing the skills gap, you also need to consider whether your organization's workloads are ready for cloud services. Most virtualized on-premises workloads were not designed for the cloud; they rely on high availability (HA) built into the infrastructure, where a failure in the environment automatically restarts the VM on a different host to maintain the workload's availability. Some organizations choose the cloud before understanding how it changes the implementation of their workloads' requirements. That's a mistake.

Before you even think about cloud, you need to understand all the requirements of your workloads — and how to support those requirements in the cloud — to help you decide whether a public cloud destination makes sense. If your workloads are mission-critical and require near-zero downtime, make sure the cloud infrastructure of choice can accommodate this HA requirement. Otherwise, make sure your technical teams have the time, resources and skills to support the requirement by rewriting the application code. The effort and time to rearchitect or refactor applications to suit public cloud infrastructure can be quite extensive.

**Ask yourself,** "What should my cloud workload roadmap for the future look like?" **And the answer should be,** "A flexible hybrid cloud that allows me to migrate, operate and manage workloads on-premises or in the public cloud and foster cloud-native innovation and modernization."

Another aspect of cloud readiness to consider is what network connectivity is required between your on-premises environment and the cloud environment. Is live migration of workloads to and from the cloud required rather than moving powered-off VMs? Do you need to maintain IP addresses when migrating workloads? Is Layer 2 connectivity needed between workloads on-premises and in the cloud? The answers to these questions depend on your organization's strategy for public cloud adoption.

### 4. Data sovereignty and security

Data sovereignty, locality and privacy requirements and regulations are a critical consideration for most organizations working across different geographies and with different vendors. Your company is responsible for navigating the requirements needed to deliver cloud services within each country to ensure your data does not cross borders in a prohibited fashion. Your public cloud provider also needs to have sufficient regional or geographic presence to meet the geographical location and data requirements.

[2] IDC's Cloud Pulse Q120, March 2020 (n=837).

Security requirements are critical, too. Traditionally, network and security teams are tasked with determining the appropriate policies and rules after a new application has been developed. This can be a time-consuming, manual and error-prone process involving various review cycles that ultimately results in a complex set of rules based on network constructs (e.g., IP addresses and ports) that are difficult to tie to applications Network-based security policies are also not conducive to changing applications. In the traditional network-centric approach to security, VLANs and hardware-based firewalls are used to channel traffic and provide a level of separation between your different workloads. This method is often used to segment your application tiers, but it does not prevent lateral communication between workloads that are in the same tier and can expose a lateral attack surface between applications. More importantly, the lifecycles of the associated policies will not be aligned with the lifecycles of the applications, leading to an explosion in the number of inspection rules and leaving you with an inadequate and inflexible security posture.

To overcome these challenges, you need to have the right level of segmentation and a security policy that is aligned with your applications so it can be provisioned and decommissioned right along with the application itself. You also need to be able to identify the application, determine which workloads compose it, and determine what network traffic is necessary for the application to function. From there you can create micro-segmentation policies to restrict any other traffic, which immediately reduces the attack surface. The cloud platform you select should enable this micro-segmentation.

### 5. Digital transformation challenges

Due to evolving business needs, geographical expansions, new product introductions, and the demands of your customers, your technology team is likely challenged with the decision about whether to keep or upgrade existing infrastructures and applications. These aren't always easy decisions to make. You need to consider countless variables such as efficiency, cost-effectiveness and available resources — and you need to decide whether to do it piecemeal or all at once. It's important that your technology team can seamlessly integrate your existing frameworks and on-premises systems built over many years without having to rebuild and replace infrastructure.

As your organization undergoes its own digital transformation, you'll want to modernize applications so you can deliver improved digital experiences to win, serve and retain your customers. These applications are driven by desired business outcomes — increased agility, innovation, growth or market differentiation — while balancing costs, security, reliability and control. The cloud plays an important role in helping your business both deliver new applications and modernize its existing ones. But modernizing existing applications in the cloud can have its challenges too, such as:

Increased costs and inability to capitalize on existing investment for modernization: Due to lack of application portability and interoperability across the hybrid environment, cloud customers are unable to move applications from on-premises to cloud environments without significant time and resources because they need to refactor their existing applications to meet the objectives of modernization.

### What is your cloud strategy? Cloud-fit or cloud-first?

The right cloud strategy helps your team focus on attaining your specific goals on the cloud journey.

- **Skill shortages in application development/delivery and infrastructure teams:** If an organization lacks the necessary skillsets, it must retrain its existing staff or hire new staff, delaying modernization projects and innovation.
- **Lack of environment integration:** Due to a fragmented technology ecosystem, organizations are unable to easily and seamlessly leverage CI/CD methodologies, application catalogs, and native cloud services to enrich enterprise applications, hindering innovation and adding costs, risk and complexity.
- **Disparate management tools, operating models and security controls:** The differences between on-premises and public cloud infrastructure limit the reuse of established management, security and governance procedures.
- **Disruption to existing business processes and operations during modernization:** Due to inflexible and inconsistent application and infrastructure architecture, there is a risk of application downtime during modernization.

To overcome these challenges, you'll want to ensure you can easily migrate workloads to the cloud, modernize those workloads in the cloud and future-proof your investment for new application development.

### 6. Investment security

Most organizations have already made significant investments in their VMware environments, running VMware® vSphere® over the last decade or so. These investments continue to offer value and payback with new hybrid cloud flexibility and are often the longest-lasting component within the data center—continuing to help drive innovation and save costs.

You'd like to continue exercising your choice of migrating applications or infrastructure elements to private, hybrid or public cloud services while reaping the benefits of on-premises investments, resources, deployments and the accumulated skills and knowledge. You'd also like to future-proof your investment with modernization capabilities to automate infrastructure operations, transform applications with containerized workloads and services, and enrich applications with native cloud services. These capabilities enable you to get the most value out of your existing investments.

## How to match public cloud with your IT modernization strategy

It's important to understand how the public cloud fits into your overall IT strategy and how far along the cloud journey you have gone to achieve the goals of your strategy. Generally, technology teams have either a cloud-fit strategy or a cloud-first strategy.

- **Cloud-fit:** Technology teams with a cloud-fit strategy are invested in their on-premises data centers — software, hardware, people, processes — and aren't necessarily looking to move everything to the public cloud today. However, they find that the public cloud gives them unique benefits that are difficult to achieve with their relatively static on-premises data centers, such as for disaster recovery. Other use cases where public cloud is advantageous are the ability to extend your data center to the cloud to access on-demand capacity, to stand up infrastructure in new geographic locations, to support business growth and to provide a more flexible development and test environment controlled by the technology team. These use cases enable you to deliver services more rapidly and easily to your customers than an on-premises solution would allow.

- Cloud-first: Technology teams with a cloud-first strategy have decided to move their on-premises infrastructure to the public cloud. They may start slowly, with just a handful of applications, or they may be more aggressive and move the entire data center to the public cloud. Their key objectives are to leverage cost-effective solutions, shift from CapEx spending to OpEx, gain flexibility and agility, and simplify infrastructure operations. These cloud-first teams are also moving to the cloud to take advantage of innovative cloud services like machine learning, Internet of Things (IoT) and data analytics and frameworks such as Kubernetes and containers to modernize their existing applications or build new applications.

Knowing which of these cloud strategies is right for your team will help you focus on the compelling use cases you want to pursue in your cloud journey. You also want to consider where you are in your cloud journey with respect to attaining your goals:

- Consideration and evolution: In this early stage, you have a chance to influence requirements as you seek out a cloud service provider. How can you benefit from cloud economics? Do you want the flexibility to move workloads bi-directionally between on-premises and the public cloud?
- Readiness and planning: In this phase, consider the timeline in which you would like to migrate to the public cloud. How can you best leverage your existing resources and skillsets?
- Migration waves: To be successful, you want to demonstrate some early wins. If you have projects with aggressive timelines, focus on moving those workloads first. For applications with low-refactoring ROI, don't waste time and effort refactoring them—follow the fastest path to move them to the cloud. Show some successful moves early on, and you will gain buy-in from stakeholders.
- Operations and optimization: Once in the cloud, leverage native cloud services and frameworks such as Kubernetes to modernize your existing applications. Make sure you have the right cloud monitoring and analytics in place.

Understanding how the cloud fits into your strategy and where you are in your cloud journey will help you pursue the compelling use cases and next steps to attain your desired outcome with the right hybrid cloud.

## Migrate and modernize without disruption: VMware Cloud on AWS

VMware Cloud on AWS delivers an infrastructure platform option for modernizing your existing enterprise applications, enabling them to handle your enterprise workloads of today and tomorrow. With VMware Cloud on AWS, you can run, monitor and manage containers and VMs on the same platform using the same tools, thereby providing flexibility and simplifying your infrastructure operations. This means you can start your modernization journey with minimal disruption to your business and rapidly migrate your applications to the cloud without downtime. Once in the cloud, you can start transforming these applications by leveraging modern frameworks such as Kubernetes, enriching them with native cloud services and automating the underlying infrastructure operations with DevOps tooling.

### Jointly engineered

VMware Cloud on AWS delivers a hybrid cloud service that integrates the familiar VMware flagship software-defined data center (SDDC) technologies of compute, storage and network virtualization (VMware vSphere, VMware vSAN™ and VMware NSX®) along with VMware vCenter Server® management and robust disaster protection and optimizes it to run on dedicated, elastic, Amazon EC2 bare-metal infrastructure. The VMware SDDC software stack is running on AWS bare-metal infrastructure, not as nested virtualization.

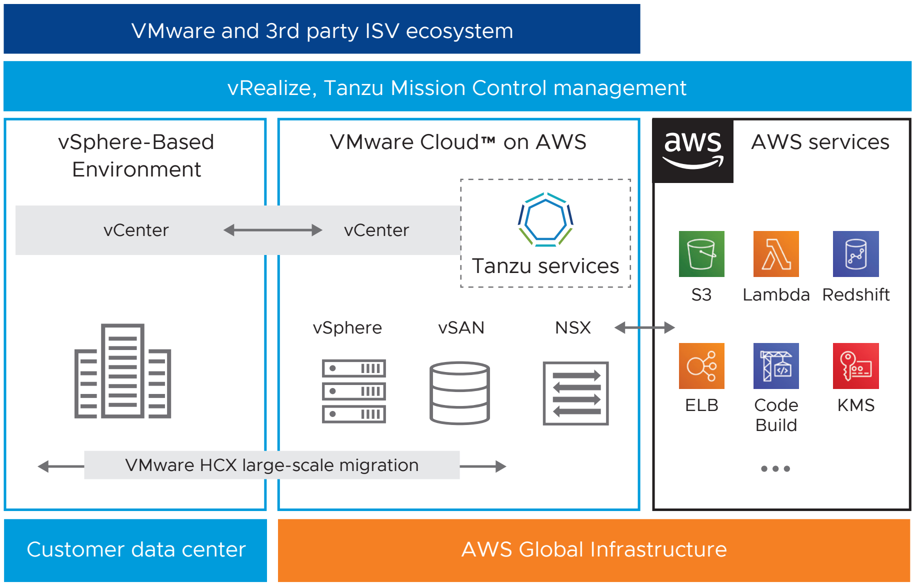

VMware and 3rd party ISV ecosystem
vRealize, Tanzu Mission Control management
vSphere-Based Environment
VMware Cloud™ on AWS
aws
AWS services
vCenter
vCenter
Tanzu services
S3
Lambda
Redshift
vSphere
vSAN
NSX
ELB
Code Build
KMS
VMware HCX large-scale migration
•••
Customer data center
AWS Global Infrastructure

**Figure 2:** VMware Cloud on AWS is a jointly engineered cloud service.

### Built on technologies you already know and use

VMware Cloud on AWS offers a platform on which you benefit from access to all the hardware resources of a host (CPU, memory, storage) versus the typical shared resource model of a public cloud. You can deploy as much as the resources allow, maximizing your existing investments. You can seamlessly integrate your existing management framework, which you've most likely built over the last several years, without having to rebuild and replace your infrastructure. Continue using familiar VMware technologies like vCenter Server — plus a broad range of third-party technology solution providers that are validated to work with VMware Cloud on AWS. Leverage vRealize® Cloud Management to deploy and operate applications, infrastructure and platform services across your hybrid cloud.

With VMware Cloud on AWS, you can run, monitor and manage containers and virtual machines on the same platform using the same tools, thereby providing flexibility and simplifying your infrastructure operations.

**IDC found that enterprise IT organizations ranked the consistent management of workflows** (provisioning, terminating, monitoring, etc.) **as the most important attribute in their hybrid cloud environments.** A lack of operational consistency between environments makes it difficult to monitor and automate processes, especially when building automations that span premises.[3]

VMware Cloud on AWS clusters can be managed from within the same vCenter and vRealize Suite of management and operations tools to create a consistent operating environment within the public cloud identical to the one in which applications would operate within the on-premises data center.

Get started with a minimum of two dedicated hosts running in the AWS cloud. Unlike a traditional public cloud approach, you won't have to worry about precisely sizing each VM because you can allocate exactly as much — or little — of key resources (compute, storage and memory) that your VM needs. You won't waste resources, need to share them, or even worry about who might be using that same hardware. The SDDC storage provided by vSAN comes with additional benefits. vSAN performs block-level deduplication and compression to save storage space. This allows you to make more efficient and cost-effective use of storage in your VMware Cloud on AWS SDDC. Additionally, vSAN support for AWS high-performance storage devices built into AWS hosts lets you get the most value from the underlying hardware.

Use the latest capabilities as you modernize your applications in the cloud. You can leverage popular and proven tools to automate hybrid cloud provisioning and management, deliver infrastructure as code-based automation for VMware Cloud on AWS, provide day-to-day and advanced operations, leverage and scale Kubernetes in the cloud to fit your needs, and support continuous integration/continuous delivery and source control. With VMware Cloud on AWS, you can take advantage of hundreds of native AWS services that leverage unique AWS capabilities, all while continuing to maintain important compatibility with your existing VMware tools. AWS Direct Connect enables you to create a high-speed, low-latency connection between your on-premises data center and AWS services including VMware Cloud on AWS. You can also ensure cloud monitoring and analytics with VMware CloudHealth®. Create a hybrid cloud-enabled management framework for today and into the future.

## Move workloads where you need them

With VMware Cloud on AWS, you can alleviate concerns about gaps in skills, time-consuming tasks, complexities associated with rewriting and refactoring workloads, and security and automation fears. The bi-directional workload portability lets you easily move your workloads to the cloud and then back on-premises as needed. This flexible, two-way approach helps you save time, power and costs and eliminate risks as well as the need to convert on-premises VMs to an entirely new format or the need to completely rewrite network, storage and security policies.

In addition, to minimize disruption to application owners and users, your migration project may require that workloads keep their IP addresses post-migration. This can be done with VMware Cloud on AWS using a Layer 2 network extension during the migration. Network extensions provide a great deal of flexibility in how a migration is performed and allow entire applications to be migrated, regardless of the layout of the underlying network addressing scheme. VMware HCX®, which is part of the VMware Cloud on AWS service, offers bi-directional application mobility across on-premises and VMware Cloud on AWS. HCX has built-in WAN optimization, deduplication and compression to increase efficiency while decreasing the time it takes to perform migrations. You can use HCX for cold, warm or live migrations as well as take advantage of replication functionality to fulfill your migration strategy.

[3] IDC technical paper sponsored by VMware, "VMware Cloud on AWS: Facilitating Agile Datacenter Extension and Virtual Desktop Infrastructure in the Public Cloud," IDC #US47164020, December 2020.

### Improved Day 2 operations

VMware Cloud on AWS is a service and therefore VMware handles all patching so you don't need to worry. This involves maintaining consistent software versions across the SDDC fleet with continuous delivery of features and bug fixes. VMware has developed automated workflows that are optimized for managing many cloud SDDCs and the service lifecycle at scale. This is largely transparent to customers using the VMware Cloud on AWS service. When VMware Cloud on AWS hosts are patched, vSphere vMotion® enables zero-downtime migration of virtual machines so that these updates can be executed transparently. You are not required to maintain N+1 capacity — the upgrade workflow will automatically provision additional resources as needed in order to support your applications without negatively impacting performance VMware is mindful of customer IT processes and ensures the minimum impact of changes.

### Are your VMs and workloads cloud-ready?

Before you think about cloud, it's important to make sure that you understand the requirements of your VMs and workloads. That will help you choose whether a cloud destination makes sense. Most virtualized workloads were never designed to run in the cloud because they cannot tolerate a failure without the capabilities that the underlying infrastructure provides, such as integrated HA. They're not immune to the impact of infrastructure lifecycle management downtime when underlying patches need to occur.

### Automated resilience

Unlike native public clouds, with VMware Cloud on AWS, you don't need to rearchitect (or replatform) your applications and availability rules to get the same resiliency you had with vSphere on-premises. A key differentiator of VMware Cloud on AWS is that availability and resiliency are designed into the service and the underlying AWS infrastructure. This enables VMware and AWS joint customers to focus on their applications and workloads rather than rethinking availability into the application layer, especially when migration and data center extension projects have stringent timelines associated with them.

### Auto remediation

VMware Cloud on AWS provides capabilities to isolate failure domains and provide automated resilience. To minimize the impact of host failures, VMware Cloud on AWS implements an Auto Remediation service that monitors every host across all customers and springs into action whenever there is a problem. The Auto Remediation service is designed to automate recovery from failed hosts, minimizing downtime and impact to customer SDDCs. Unlike in an on-premises deployment, there is no need to maintain hot spares in the cloud. VMware and AWS jointly manage the pool of instances in every Region and Availability Zone to ensure Auto Remediation has sufficient spare capacity to automatically replace a faulty host with a healthy new one. This happens without the need for customer intervention. vSphere HA ensures the availability of VMs by restarting them on healthy hosts within the cluster if a host failure occurs.

In addition to VM and host-level failure recovery, Stretched Clusters for VMware Cloud on AWS protect you against an AWS Availability Zone failure. Applications can span two AWS Availability Zones within a VMware Cloud on AWS cluster. If an Availability Zone experiences an outage or degradation, VMs will be restarted on hosts in the other Availability Zone.

## Modernize applications in the cloud

VMware Cloud on AWS provides a fast path to migrate your applications to the public cloud without downtime or having to refactor and rearchitect them. Once in the cloud, you can determine the best modernization path for each application with minimal disruption to your business. Extend the value of enterprise applications running in VMware Cloud on AWS with simple access to hundreds of native AWS services. By seamlessly integrating with these innovative native AWS services, you can incrementally enrich your applications and enhance the end user experience. Key AWS services cover aspects of storage, networking, content delivery, database, analytics, serverless data processing, security, IoT, artificial intelligence (AI) and machine learning.

## Key capabilities

### Automate infrastructure operations

- Embrace infrastructure as code, GitOps and infrastructure pipelines
- SDK, RESTful API and CLI in-product developer center

### Transform applications with Kubernetes

- Automation and operations for containers and VMs in the same platform
- VMware Tanzu Kubernetes Grid support
- Centralized management and governance for Kubernetes with Tanzu Mission Control
- Agile development with VMware Pivotal Labs
- CI/CD ecosystem support

### Enrich with cloud services

- Direct access to AWS services
- Access to VMware partner-ready solutions

Your organization can also start transforming applications by leveraging modern frameworks such as Kubernetes and automating the underlying infrastructure operations with DevOps tooling. With VMware Cloud on AWS, you can run, monitor and manage containers and virtual machines on the same platform using the same tools. This provides flexibility and simplifies your infrastructure operations so you'll be able to run today's workloads into the future.

### Containers and Kubernetes

Organizations that want to start running containers and Kubernetes on VMware Cloud on AWS can get started right away. VMware Tanzu™ Kubernetes Grid™ support for VMware Cloud on AWS enables you to deploy your SDDC in the cloud, with the required components needed to deploy and scale Kubernetes infrastructure to fit your needs.

Tanzu Kubernetes Grid is an enterprise-ready Kubernetes distribution that packages open-source technologies and automation tooling to help get you up and running quickly with a scalable, multicluster Kubernetes environment. Those teams deploying Tanzu Kubernetes Grid on VMware Cloud on AWS can benefit from 24x7 break-fix support for Kubernetes and key open-source ecosystem technologies. Additionally, they can also engage with VMware Tanzu Labs for help transforming applications and leveraging modern application development and delivery methodologies. What's more, Tanzu Mission Control support for VMware Cloud on AWS provides a centralized management platform for consistently operating and securing your Kubernetes infrastructure and modern applications across multiple teams and clouds. Customers who are running Kubernetes workloads on VMware Cloud on AWS can attach their Kubernetes clusters to Tanzu Mission Control for centralized management, whether it is a Tanzu Kubernetes Grid cluster, DIY clusters, or other Cloud Native Computing Foundation (CNCF)-conformant Kubernetes clusters. After attaching clusters to Tanzu Mission Control, customers can gain a centralized view of all their Kubernetes clusters and workloads running on VMware Cloud on AWS for quickly identifying and troubleshooting issues and can leverage Tanzu Mission Control's uniquely designed capabilities such as policy engine, cluster inspection and data protection to efficiently and securely manage their Kubernetes clusters and modern apps at scale. This establishes a reliable foundation for cloud-native application management and application modernization.

### Leverage the power of automation

To help customers leverage automation, VMware Cloud on AWS provides high level cmdlets for PowerCLI and infrastructure as code (IaC) for your key infrastructure management workflows. vRealize Automation Cloud can deliver infrastructure as code-based automation for VMware Cloud on AWS through its blueprints, which are written declaratively in YAML. With GitLab and GitHub integration, the YAML blueprints can be subject to source control management, with versioning synchronized between blueprints and the source control system. Additionally, the Hashicorp Terraform provider for VMware Cloud on AWS enables your cloud admins and DevOps engineers to declaratively define and provision VMware Cloud on AWS environments and simplify the management of hybrid infrastructure through automation. This can be used with the existing Terraform providers for vSphere and NSX to manage end-to-end hybrid infrastructure from SDDC networking to VM lifecycle. Furthermore, AWS CloudFormation templates can be used to create and deploy a VMware Cloud on AWS SDDC. As you can see, there are several options to choose for automating infrastructure operations for your hybrid cloud.

> Migrate your applications to VMware Cloud on AWS and then transform, enrich and automate your applications and infrastructure operations.

Customers can leverage the VMware Cloud Marketplace for a vast ecosystem of VMware Cloud-ready solutions for continuous integration/continuous delivery (CI/CD) and source control. VMware Code Stream supports VMware Cloud on AWS and provides powerful infrastructure release pipeline automation capabilities for rapidly, safely and consistently delivering the infrastructure that developers and lines of business (LoBs) need to be productive. VMware Cloud on AWS also enables the deployment and usage of the popular third-party ISV CI/CD utilities such as Jenkins Virtual Appliance, GitLab Community Edition, JFrog, and Xebia Labs. VMware Cloud on AWS supports the deployment of virtual appliances for both GitLab Community Edition and Subversion for source control of code-based contributions.

These modernization, automation and DevOps capabilities for CI/CD and source control enable your organization to modernize and future-proof existing applications. VMware Cloud on AWS forms a key part of the overall tool set and services that VMware offers to help customers with the transformation of their application portfolio.

### Protect your investments and leverage existing skillsets

Your existing resources and investments in VMware offer you the greatest choice and most flexible hybrid cloud future, which are all based on mature, trusted and proven technologies. With VMware Cloud on AWS, you don't need to reinvest in brand new technologies. You can easily expand your existing environment to the cloud with minimal disruption.

Having vCenter on-premises and in the cloud's SDDC delivers consistency in operations between environments, reducing the need to retrain staff. IT teams can leverage a familiar, single pane of glass with Hybrid Linked Mode to manage their workloads. Hybrid Linked Mode allows you to link your VMware Cloud on AWS vCenter Server instance with your on-premises instance so you can view and manage the inventories of both your on-premises and VMware Cloud on AWS SDDCs from a single vSphere Client interface, accessed using your on-premises credentials.

IDC calculates that, on average, organizations using VMware Cloud on AWS incur total migration-related costs that are 57% lower than those of other public cloud solutions. The efficiencies and cost savings translate into an average savings of $233,900 per 100 VMs, reflecting a much lower cost approach to migrating workloads to the public cloud.

### Application modernization benefits

- **Minimize disruption:** Migrate and modernize.
- **Provide portability**: Optimize app placement as needed.
- **Abstract complexity**: Infrastructure provides resiliency.
- **Empower IT**: Access DevOps-ready platform and services.

**200+**

AWS services, including AI/ML, analytics, IoT and more

**300+**

partner-ready solutions across DevOps, migration, monitoring and more

Faster and lower cost to migrate to VMware Cloud on AWS vs. native public cloud

57%

Save 57% by eliminating costly rework and refactoring.[4]

## Secure your data everywhere it exists

VMware Cloud on AWS provides the ability to run, manage and secure your applications in a seamlessly integrated hybrid IT environment. Your production applications require advanced networking and security services including micro-segmentation, which VMware NSX-T enables as part of VMware Cloud on AWS.

### Distributed firewall

The ability to do micro-segmentation with a distributed firewall is one of the key features of VMware Cloud on AWS. Not only does it provide you with an easy way to create sophisticated security policies, but it also allows these policies to be applied to even a small cluster without any extra networking components or devices.

What's unique about a distributed firewall is that it has contextual view of the virtual data center. This means the distributed firewall can secure workloads based on VM criteria instead of just source and destination IP addresses. Traditional firewalling is based on source and destination IPs—constructs that have no business logic or context into applications. VMware's distributed firewall secures workloads based on smarter criteria, such as the name of the virtual machine or metadata. This enables you to build security rules that are based on business logic using tags or naming conventions. Properly done, they can specify a physical location, business application, and whether a workload is test, development or production. Using a distributed firewall, you can have east-west firewalling within the data center and achieve micro-segmentation and ultimately reduce the impact of a potential security breach and achieve compliance targets.

### Doubling down on security and compliance

VMware Cloud on AWS inherits all the physical and network protections of the AWS infrastructure and adds dedicated compute and storage along with the security capabilities built into vSphere, vSAN and NSX. All data transmitted between your on-premises data center and the service can be encrypted via VPN. All data between the VMware Cloud on AWS service and your SDDCs is encrypted, and data at rest is encrypted. The VMware Cloud on AWS infrastructure is monitored and regularly tested for security vulnerabilities and hardened to enhance security.

VMware Cloud on AWS GovCloud (U.S.) is a secure platform for government agencies to access the benefits of public and private clouds to further increase agility and security. It enables you to seamlessly and securely integrate a hybrid cloud offering that aligns with U.S. public sector agency strategy.

VMware continuously monitors your existing and emerging security standards and requirements and integrates applicable requirements into their cloud service compliance programs. VMware Cloud on AWS has achieved a number of industry-leading compliance certifications and is able to support a wide variety of customer use cases and compliance requirements. VMware's compliance offerings cover a wide range of global certifications from ISO 27001/17/18 certifications to various region-specific

[4] IDC technical paper sponsored by VMware, "The Business Value of Running Applications on VMware Cloud on AWS in VMware Hybrid Cloud Environments," IDC #US46919520, October 2020.

certifications covering North America, EMEA, and Asia Pacific regions. VMware Cloud on AWS now offers PCI DSS compliant SDDCs that can drastically simplify the tasks to achieve and maintain PCI DSS compliance. You can now migrate your applications that process, store, or transmit cardholder data to VMware Cloud on AWS SDDC. VMware has also published several compliance technical papers addressing the various regional governmental and financial services industry compliance requirements. In addition, VMware Cloud on AWS has a strong global presence worldwide to help you address data sovereignty or locality needs. Please check out regional availability here.

## Think of cloud as a strategy, not a destination

Today's approach to the cloud can shift quickly as requirements change. In such a volatile world—where every change often winds up costing you a lot of extra time, resources and money—VMware's approach to cloud is to empower a long-term strategy that lets you take your existing on-premises investments and seamlessly create a hybrid architecture to leverage the public cloud. The result is speed, flexibility, choice and no lost investments.

Each public cloud provider takes a unique approach to building its underlying compute, storage and networking infrastructure, and it usually requires certain cloud optimizations or adaptations for the applications to work properly in the public cloud infrastructure. This makes the public cloud incompatible with your on-premises environment and forces you to replatform or refactor your applications in order to move them to the public cloud. VMware enables the seamless movement of workloads between on-premises and the public cloud with the fastest path possible (without any refactoring) so you can rapidly realize the benefits of the public cloud while maintaining the flexibility to move those workloads back on-premises as needed.

## Cloud strategy use cases

VMware Cloud on AWS provides a seamlessly integrated hybrid cloud offering addressing use cases that align to your cloud strategy:

- Application-specific cloud migration—Move specific applications to the cloud based on your particular business needs such as cost savings, availability, scalability, proximity to native public cloud services, performance, data sovereignty, security or manageability.
- Footprint expansion or on-demand capacity—Leverage the public cloud for your geographic capacity needs (e.g., data sovereignty rules or to be closer to end users) or temporary capacity without having to invest in building out a new data center. Handle seasonal spikes in demand and be able to perform test and development activities in a cloud environment that is operationally similar to on-premises environments.
- Virtual desktops and published apps in the cloud—Easily add and extend your on-premises desktop services without buying additional hardware. Co-locate virtual desktops or published applications near latency-sensitive applications in the cloud. Leverage elastic capacity as a cost-effective way to protect your on-premises VMware Horizon deployments or for temporary needs.

### Learn more

vmware.com/products/vmc-on-aws

To find out more about migrating workloads to VMware Cloud on AWS, visit vmc.techzone.vmware.com/cloud-migration

- **Disaster recovery (DR) as a service**—Replace or retire your existing DR solution and optimize DR costs with on-demand failover capacity and Pilot Light (a small subset of SDDC hosts deployed ahead of time) for faster recovery times. Mitigate compliance risks with automated health checks and prepare for rapid ransomware recovery.
- **Application modernization**—Use cloud-scale infrastructure and services to extend the value of your existing enterprise applications and ensure consistent infrastructure compatibility with your on-premises environments. Build new applications using native AWS services while leveraging infrastructure that is consistent with your on-premises environments.

## Conclusion

Nearly every enterprise is using the public cloud in some fashion, with the majority opting for a hybrid cloud solution. Organizations recognize the benefit of having the public cloud integrate and work seamlessly with their on-premises infrastructure while taking advantage of their existing teams, skillsets, tools and processes. This enables your technology team to manage multiple environments with one tool set and eliminate the need to learn (or additionally hire for) different tools, management frameworks, platforms, processes, security policies and more. They can migrate applications from a private cloud to a public cloud and vice versa.

The use of VMware Cloud on AWS for your hybrid cloud provides compelling TCO and investment protection, and it allows you to maximize the use of existing skills, tools and processes. VMware Cloud on AWS also supports established governance and security policies and provides access to native cloud services and support for frameworks such as Kubernetes to modernize your existing applications. Additionally, you gain enterprise-grade capabilities including availability, performance, manageability and security. No matter where you are in your cloud journey with respect to attaining your cloud-fit or cloud-first goals, VMware Cloud on AWS is an optimal solution when it comes to leveraging hybrid cloud and modernizing and future-proofing your existing applications.

Item No: Put the Hybrid Cloud to Work for You - VMware Cloud on AWS 1/23